UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,737	08/03/2001	Fumihikko Sano	212288US2S	5068

22850 7590 01/19/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/920,737	SANO, FUMIHIKKO	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20030529*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: The specification appears to contain minor errors such as typographical errors and uncommon idiomatic expressions. For example, on page 22, line 27-page 23, line 1, it appears that "storage medium S" is intended to read "storage medium SM", and on page 1, lines 17-21, the sentence is generally awkwardly phrased, especially "in the field of a computers" and "there is widely known a cipher technique".

Appropriate correction is required. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Drawings

2. Figure 7 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.121(d)) so as not to obstruct

any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claims 3 and 5 objected to because of the following informalities: Claim 3 recites the limitation "plain data" in lines 5-6 of the claim. It appears that this is intended to read "plain text data". Claim 5 recites the limitation "by convert a common key" in line 9 of the claim. It appears that this is intended to read "by converting a common key". Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 3, 5, 7, 9, 11, 13, and 15 each recite the limitation "in accordance with each block", in lines 5 and 7 of claim 1, lines 5 and 7 of claim 3, line 7 of claim 5, line 7 of claim 7, lines 7-8 of claim 9, lines 9-10 of claim 11, lines 3-4 and 6-7 of claim 13, and

lines 5-6 of claim 15. It is unclear to what "each block" is intended to refer, whether to blocks of data or to, for example, the "encryption function portions" of claim 1. This renders the claims indefinite. For purposes of interpreting the prior art, it is assumed that "each block" is intended to refer to blocks of data.

Further, Claims 1, 3, and 9 each recite the limitation "and/or", in line 5 of claim 1, line 5 of claim 3, and line 8 of claim 9. The inclusion of this limitation renders the scope of the claims indefinite, as it is unclear which of the listed limitations are necessarily within the scope of the claim. For example, in Claim 1, it is unclear whether the encryption function portions can either only be provided in parallel, only output cipher text data, or only output plain text data, or whether the encryption function portions must be provided in parallel, and both output cipher text data and plain text data.

Additionally, Claims 1, 3, 5, 7, 9, and 11 each recite the limitation "any one of two or more types of conversion processing different from each other", in lines 11-12 in each of claims 1, 3, 5, and 7, and in lines 15-16 of claims 9 and 11. Similarly, Claims 13 and 15 each recite the limitation "any one of a plurality of types of conversion processing" in lines 11-12 of claim 13 and lines 9-10 of claim 15. These limitations render the claims indefinite, as the claims could be interpreted as each of the key generation means or steps having the same one type of conversion processing. That is, the claims could read that exactly one type of conversion processing is selected, or the claims could read on one type of conversion processing being chosen for each key generation means or step, which makes the scope of the claims unclear.

Further similarly, Claims 2, 4, 6, 8, 10, and 12 each recite the limitation "any one of two or more variable data different from each other", in lines 3-4 of each claim, and Claims 14 and 16 each recite the similar limitation "any one of a plurality of variable data" in lines 3-4 of each claim. As above, these limitations render the claims indefinite, as the claims could be interpreted as each conversion processing being based on the same one variable data. The claims could also be interpreted as a different variable data being chosen for each conversion processing. This renders the scope of the claims unclear.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 3, 9, and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by applicant admitted prior art.

In reference to Claims 1 and 3, Applicant discloses that the prior art teaches an encryption/decryption apparatus including a plurality of encryption function portions in parallel to each other which are used to encrypt plain text into cipher text or decrypt

cipher text into plain text based on a key (Prior Art Figure 1, Encryption functions F) and a plurality of key data generating portions (or means) which generate key data by converting a common key (Key K) based on an intermediate processing result (i_1-i_{m-1} and s_1-s_{m-1}) and any one conversion processing (Conversion functions f).

Claim 9 is directed to a software implementation of the apparatus of Claim 1, and is rejected by a similar rationale.

Claim 13 is directed to a method corresponding substantially to the apparatus of Claim 1, and is rejected by a similar rationale.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2, 4, 10, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Johnson et al, US Patent 5796830.

The applicant admitted prior art discloses everything as applied to Claims 1, 3, 9, and 13 above. However, the admitted prior art does not explicitly disclose that the conversion processing converts the common key based on any one variable data.

Johnson discloses a system in which a key is combined with a salt, which is a random variable used to increase randomness (column 12, lines 4-14). Johnson further discloses that a value to be encrypted can be divided into blocks, and a different salt chosen for each block (column 17, lines 42-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption apparatus, software, and method of the prior art to include converting a key based on a variable data, in order to increase the randomness provided (see Johnson, column 12, lines 4-14).

10. Claims 5, 7, 11, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Schneier, *Applied Cryptography*.

In reference to Claims 5 and 7, Applicant discloses that the prior art teaches an encryption apparatus including a plurality of encryption function portions in parallel to each other which are used to encrypt plain text into cipher text based on a key (Prior Art Figure 1, Encryption functions F) and a plurality of key data generating portions (or means) which generate key data by converting a common key (Key K) based on an intermediate processing result (i_1-i_{m-1} and s_1-s_{m-1}) and any one conversion processing (Conversion functions f). However, the prior art disclosed by Applicant does not explicitly disclose generating an authenticator based on cipher text data generated by an encryption function.

Schneier discloses that a Message Authentication Code (MAC) can be generated using any keyed hash function such as a block cipher operating in cipher block chaining (CBC) mode (page 456, "CBC-MAC"). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the prior art encryption apparatus to be used in generating an authenticator such as a MAC, in order to provide authenticity without secrecy (see Schneier, page 455, section 18.14).

Claim 11 is directed to a software implementation of the apparatus of Claim 1, and is rejected by a similar rationale.

Claim 15 is directed to a method corresponding substantially to the apparatus of Claim 1, and is rejected by a similar rationale.

11. Claims 6, 8, 12, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Schneier as applied to claims 5, 7, 11, and 15 above, and further in view of Johnson.

The combination of admitted prior art and Schneier discloses everything as applied to Claims 5, 7, 11, and 15 above; however, the combination does not explicitly disclose that the conversion processing converts the common key based on any one variable data.

Johnson discloses a system in which a key is combined with a salt, which is a random variable used to increase randomness (column 12, lines 4-14). Johnson further discloses that a value to be encrypted can be divided into blocks, and a different salt

chosen for each block (column 17, lines 42-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption apparatus, software, and method of the prior art, used to generate an authenticator as taught by Schneier, to include converting a key based on a variable data, in order to increase the randomness provided (see Johnson, column 12, lines 4-14).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Hardy et al, US Patent 5230020, disclose a key management system that includes several different key generators.

b. Bellare et al, US Patent 5673319, disclose a block cipher, used to generate a CBC-MAC, which includes variable inputs as initialization vectors.

c. Candelore et al, US Patent 6061449, disclose a chaining block cipher that includes block reordering and random numbers.

d. Luyster, US Patent 6182216, discloses a block cipher including varying subkeys.

e. Coppersmith et al, US Patent 6185304, disclose a block cipher supporting variable keys and rounds.

f. Jakubowski et al, US Patent 6226742, disclose a block cipher for generating a MAC.

g. Djakovic, US Patent 6351539, discloses a cipher with random numbers mixed into the ciphering.

h. Tan, US Patent 6490353, discloses a block cipher that includes selecting between multiple cryptographic algorithms for each block.

i. *SKIPJACK and KEA Algorithm Specifications* disclose the SKIPJACK algorithm, which includes combining plaintext, keys, and a counter variable.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER